Chapter A:

Introductory matters

Version ~~4~~5.0, November ~~2022~~2023

Contents

Purpose

A.1 The Australian Information Commissioner issues these Privacy Safeguard guidelines under paragraph 56EQ(1)(a) of the *Competition and Consumer Act 2010* (Competition and Consumer Act). These guidelines are not a legislative instrument.[1]

A.2 The Privacy Safeguard guidelines are made in order to guide entities on avoiding acts or practices that may breach the privacy safeguards, which are set out in Division 5 of Part IVD of the Competition and Consumer Act.

A.3 Part IVD of the Competition and Consumer Act is the legislative base for the consumer data right (CDR) system.

A.4 The Privacy Safeguard guidelines outline:

- the mandatory requirements in the privacy safeguards and related consumer data rules (CDR Rules) — generally indicated by 'must' or 'is required to'
- the Information Commissioner's interpretation of the privacy safeguards and CDR Rules — generally indicated by 'should'
- examples that explain how the privacy safeguards and CDR Rules may apply to particular circumstances. Any examples given are not intended to be prescriptive or exhaustive of how an entity may comply with the requirements in the privacy safeguards; the particular circumstances of an entity will also be relevant, and
- good privacy practice to supplement minimum compliance with the mandatory requirements in the privacy safeguards and CDR Rules — generally indicated by 'could'.

A.5 The Privacy Safeguard guidelines are not legally binding and do not constitute legal advice about how an entity should comply with the privacy safeguards and CDR Rules. An entity may wish to seek independent legal advice where appropriate.[2]

A.6 In developing the Privacy Safeguard guidelines, the Information Commissioner has had regard to the objects of Part IVD of the Competition and Consumer Act, stated in section 56AA of the Competition and Consumer Act:

- to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed safely, efficiently and conveniently:
  - to themselves for use as they see fit, or
  - to accredited persons for use subject to privacy safeguards
- to enable any person to efficiently and conveniently access information in those sectors that is about goods (such as products) or services and does not relate to any identifiable, or reasonably identifiable, consumers, and
- to create more choice and competition, or to otherwise promote the public interest.

[1] Competition and Consumer Act, subsection 56EQ(5).

[2] Further, if there is an inconsistency between the Privacy Safeguard guidelines and the CDR Rules, the rules prevail over the guidelines to the extent of the inconsistency: Competition and Consumer Act, subsection 56EQ(4).

About the consumer data right

A.7 The CDR aims to provide greater choice and control for Australians over how their data is used and disclosed. It allows consumers to access particular data in a usable form and to direct a business to securely transfer thatparticular data in a usable form to an accredited person or other permitted person under the CDR rules.

A.8 Individual consumers and small, medium and large business consumers are able to exercise the CDR in relation to data that is covered by the CDR system.

A.9 The CDR commenced in the banking sector in 2019 (known as 'Open Banking') and will commence in the energy sector in 2022.[3] (with staged application to continue into 2024).[4]Next, CDR will be implemented in the telecommunicationsnon-bank lending sector,[5] and will continue to be introduced across the broader economy as designated by the Minister.[6]

About the privacy safeguards

A.10 The privacy safeguards are legally binding statutory provisions, which ensure the security and integrity of the CDR system. The specific requirements for certain privacy safeguards are set out in the CDR Rules.

A.11 The privacy safeguards set out standards, rights and obligations in relation to collecting, using, disclosing and correcting CDR data for which there are one or more CDR consumers:

- Privacy Safeguard 1 – Open and transparent management of CDR data
- Privacy Safeguard 2 – Anonymity and pseudonymity
- Privacy Safeguard 3 – Soliciting CDR data from CDR participants
- Privacy Safeguard 4 – Dealing with unsolicited CDR data from CDR participants
- Privacy Safeguard 5 – Notifying of the collection of CDR data
- Privacy Safeguard 6 – Use or disclosure of CDR data by accredited data recipients or designated gateways
- Privacy Safeguard 7 – Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways
- Privacy Safeguard 8 – Overseas disclosure of CDR data by accredited data recipients

[3] For staged application of CDR Rules in the energy sector, see CDR Rules, Part 8 of Schedule 4. For further information about staged application of CDR Rules, see Chapter B (Key concepts).

[4] For staged application of CDR Rules in the energy sector, see CDR Rules, Part 8 of Schedule 4. For further information about staged application of CDR Rules, see Chapter B (Key concepts).

[5] The telecommunications sector was designated on 24 January 2022. See the Consumer Data Right (Telecommunications Sector) Designation 2022. See Chapter B (Key concepts) for additional information about designation instruments.

[6] For more information about the rollout of the CDR, see https://www.cdr.gov.au/rollout.

- Privacy Safeguard 9 – Adoption or disclosure of government related identifiers by accredited data recipients
- Privacy Safeguard 10 – Notifying of the disclosure of CDR data
- Privacy Safeguard 11 – Quality of CDR data
- Privacy Safeguard 12 – Security of CDR data, and destruction or de-identification of redundant CDR data
- Privacy Safeguard 13 – Correction of CDR data

A.12 The privacy safeguards only apply to CDR data for which there are one or more 'CDR consumers'.[7] A CDR consumer can be an individual or a business enterprise.[8]

A.13 There are a number of factors that determine whether CDR data has a 'CDR consumer'.[9] In particular, for CDR data to have a CDR consumer, at least one person needs to be identifiable or reasonably identifiable from the CDR data or other information held by the relevant entity.[10] See Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines for the full meaning of 'CDR consumer'.

A.14 The privacy safeguards do not apply where there is no CDR consumer[11] because, for example, there is no person that is identifiable or reasonably identifiable from the data. Product data is an example of CDR data for which there is no CDR consumer.

A.15 The privacy safeguards are structured to reflect the CDR data lifecycle. They are grouped into five subdivisions within Division 5 of Part IVD of the Competition and Consumer Act:

- Subdivision B — Consideration of CDR data privacy (Privacy Safeguards 1 and 2)
- Subdivision C — Collecting CDR data (Privacy Safeguards 3, 4 and 5)
- Subdivision D — Dealing with CDR data (Privacy Safeguards 6, 7, 8, 9 and 10)
- Subdivision E — Integrity of CDR data (Privacy Safeguards 11 and 12)
- Subdivision F — Correction of CDR data (Privacy Safeguard 13)

A.16 The requirements in each of these privacy safeguards interact with and complement each other.

A.17 The privacy safeguards extend to certain acts, omissions, matters and things outside Australia.[12]

---

[7] Competition and Consumer Act, subsection 56EB(1).

[8] Competition and Consumer Act, subsection 56AI(3); Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraphs 1.100 and 1.101. See also *Acts Interpretation Act 1901* (Cth), section 2C, which provides that in any Act (including the references to 'person' in the Competition and Consumer Act, subsection 56AI(3)), expressions used to denote persons generally include a body politic or corporate as well as an individual.

[9] Competition and Consumer Act, subsection 56AI(3).

[10] Competition and Consumer Act, paragraph 56AI(3)(c). The 'relevant entity' here is the data holder, accredited data recipient, or person holding data on their behalf: Competition and Consumer Act, subsection 56AI(3)(c)(ii) referencing subsection 56AI(3)(b).

[11] Competition and Consumer Act, subsection 56AI(3)(c).

[12] Competition and Consumer Act, subsection 56AO(1). In particular, the Privacy Safeguards apply for CDR data held inside Australia (subsection 56AO(2)), acts or omissions by (or on behalf of) an Australian person (paragraph 56AO(3)(a)),

A.18 In respect of CDR data held within Australia, the privacy safeguards apply to all persons, including foreign persons.[13]

A.19 In respect of an act or omission relating to CDR data held outside Australia, the privacy safeguards only apply if the act or omission:[14]

- is done by or on behalf of an Australian person
- occurs wholly or partly in Australia, or wholly or partly on board an Australian aircraft or an Australian ship, or
- occurs wholly outside Australia, and an Australian person suffers, or is likely to suffer, financial or other disadvantage as a result of the act or omission.

How to use these guidelines

A.20 The structure of the Privacy Safeguard guidelines reflects the structure of the privacy safeguards: Privacy Safeguards 1 to 13 are each dealt with in separate chapters.

A.21 The number of the chapter corresponds to the number of the privacy safeguard.

A.22 Chapter B contains guidance on general matters, including an explanation of key concepts that are used throughout the privacy safeguards and the Privacy Safeguard guidelines.

A.23 Chapter C contains guidance on consent, which is the primary basis for collecting, using and disclosing CDR data under the CDR system.

A.24 These guidelines should be read together with the full text of Division 5 of Part IVD of the Competition and Consumer Act and the CDR Rules.

Who must comply with the privacy safeguards?

A.25 The privacy safeguards apply to the following entities who are authorised or required under the CDR system to collect, use or disclose CDR data for which there is at least one CDR consumer:

- **accredited persons:** persons who have been granted accreditation (at either the unrestricted or sponsored level)[15] by the Australian Competition and Consumer Commission (ACCC) to receive data through the CDR system[16]
- **accredited data recipients:** accredited persons who have collected the CDR data from a data holder or another accredited data recipient[17]

---

acts or omissions occurring wholly or partly in Australia or on board an Australian aircraft or ship (paragraph 56AO(3)(b)), or acts or omissions occurring wholly outside Australia if an Australian person suffers or is likely to suffer financial or other disadvantage as a result of the act or omission (paragraph 56AO(3)(c)).

[13] Competition and Consumer Act, subsection 56AO(2).

[14] Competition and Consumer Act., subsection 56AO(3).

[15] CDR Rules, rule 5.1A. Persons accredited at the sponsored level are known as 'affiliates'.

[16] For specific requirements, see Competition and Consumer Act, section 56CA.

[17] For specific requirements, see Competition and Consumer Act, section 56AK.

- **data holders:** persons who hold data specified in a designation instrument and meet relevant conditions in the Act, who may be required to disclose data under the CDR system (including primary and secondary data holders for shared responsibility data),[18] and
- **designated gateways:** entities designated by the Minister as responsible for facilitating the transfer of information between data holders and accredited persons.[19]

A.26 Each of these types of entities are defined in the Competition and Consumer Act and discussed further in Chapter B (Key concepts).

A.27 Each privacy safeguard chapter specifies the type of entity to which it applies.

Additional roles for accredited persons

A.28 Some accredited persons perform specific roles in the CDR system. This includes some roles under a sponsorship arrangement, a CDR representative arrangement, or an outsourced service provider arrangement.

A.29 The sponsored accreditation model allows a person accredited to the 'sponsored' level (an 'affiliate') to provide goods or services directly to a consumer where the affiliate has a sponsorship arrangement with an unrestricted accredited person (a 'sponsor').[20] The model is intended to provide an alternative to unrestricted accreditation and support a broader array of business arrangements in the CDR system.[21] The two roles for accredited persons under this model are:

- **Affiliates:** persons who have entered into a written contract, known as a sponsorship arrangement, with another person with unrestricted accreditation (known as the sponsor).[22] Affiliates are accredited to the sponsored level, must comply with the privacy safeguards and are liable in their own right for their handling of CDR data.
- **Sponsors:** persons who have entered into a written contract, known as a sponsorship arrangement, with another person (known as the affiliate) under which the sponsor discloses CDR data they hold as an accredited data recipient to the affiliate.[23] Sponsors are accredited to the unrestricted level and must continue to comply with the privacy safeguards when acting at their affiliate's request.

Both sponsors and affiliate are required to comply with the privacy safeguards when handling CDR data.

A.30 The CDR representative model allows an unaccredited person (a 'CDR representative') to use or disclose CDR data to provide CDR goods or services directly to a consumer, where they have a CDR representative arrangement with an unrestricted accredited person (a 'CDR

[18] At a high level, these conditions are that the person is also designated, that the person is a reciprocal data holder, or that the person meets certain conditions in the rules. For specific requirements, see Competition and Consumer Act, section 56AJ. For definitions of primary and secondary data holders, see CDR Rules, subrule 1.7(1).

[19] For specific requirements, see Competition and Consumer Act, subsection 56AL(2).

[20] CDR Rules, rule 1.10D.

[21] See Chapter B (Key concepts) for additional information about sponsorship arrangements, sponsors and affiliates.

[22] CDR Rules, rule 1.10D.

[23] CDR Rules, rule 1.10D.

representative principal').[24] As with sponsored accreditation, the CDR representative model is intended to facilitate the participation of a broader array of business models in the CDR system.[25] The role for accredited persons under this model is:

- **CDR representative principal:** persons who have entered into a CDR representative arrangement with a person without accreditation, known as 'the CDR representative'. CDR representative principals are accredited to the unrestricted level, collect CDR data on behalf of their CDR representative and are liable for the actions of the CDR representative.[26]

A.31 A CDR outsourcing arrangement allows an accredited or unaccredited outsourced service provider (an 'OSP') engaged by an accredited person (a 'principal') to do one or both of the following:

- collect CDR data from a CDR participant on behalf of the OSP chain principal
- provide goods or services to the principal using CDR data that the OSP collected on the principal's behalf or that was disclosed to the OSP by that principal.[27]

The two roles for accredited persons under this type of arrangement are:

- **Accredited outsourced service providers (OSPs):** accredited entities who collect CDR data on behalf of a principal, or provide goods or services to the principal under a CDR outsourcing arrangement.[28] ~~There is no requirement for OSPs to be accredited, but some accredited entities may choose to enter a CDR outsourcing arrangement in a provider capacity.~~ All OSPs (whether accredited or unaccredited) must comply with the terms of their written contract with the principal that engaged them. An accredited OSP must also comply with the privacy safeguards.
- **Principals under a CDR outsourcing arrangement:** accredited entities who engage an OSP under a CDR outsourcing arrangement.[29] Principals who are 'chain principals'[30] are liable for any collection, use or disclosure of service data by their OSP or their OSP's subcontractors.[31]

A.32 Each of these specific roles is discussed further in Chapter B (Key concepts).

---

[24] CDR Rules, rule 1.10AA.

[25] See Chapter B (Key concepts) for additional information about CDR representative arrangements, CDR representative principals and CDR representatives.

[26] As unaccredited entities, 'CDR representatives' are discussed below under the 'CDR system roles for unaccredited entities' heading.

[27] CDR Rules, subrule 1.10(~~2~~3)(a).

[28] While there is no requirement for an OSP to be accredited under the CDR system, some accredited persons may choose to enter a CDR outsourcing arrangement in a provider capacity.

[29] CDR Rules, rule 1.10.

[30] An 'OSP chain principal' is the initial OSP principal entity in a chain of CDR outsourcing arrangements – see 'Outsourcing' in Chapter B: Key concepts for more information.

[31] CDR Rules, rule 1.16. Principals who are not 'chain principals' do not carry this liability. For further discussion of subcontracting under a further outsourcing arrangement, see the discussion under 'Outsourced service provider' in Chapter B (Key concepts).

CDR system roles for unaccredited entities

A.33 In specified circumstances, an entity who is not an accredited person, accredited data recipient, data holder or designated gateway can handle CDR data within the CDR system. These entities are not directly bound by the privacy safeguards set out in Division 5 of Part IVD of the Competition and Consumer Act. This includes entities performing the following roles:

- **CDR representative:** further to the discussion of the CDR representative model in paragraph A.30A.30 above, a CDR representative is a person who has entered into a CDR representative arrangement with a CDR representative principal under which they can use or disclose CDR data to provide CDR goods or services directly to a consumer. As unaccredited entities, CDR representatives are not directly bound by the privacy safeguards, but must comply with the terms of their written contract with their CDR representative principal. These contractual obligations apply in addition to other privacy obligations a CDR representative will have under the *Privacy Act 1988* (Privacy Act) if they are an APP entity.
- **Unaccredited outsourced service provider: (OSP):** further to the discussion of CDR outsourcing arrangements in paragraph A.31, an unaccredited OSP is an unaccredited person who collects CDR data from a CDR participant on behalf of aan OSP chain principal under a CDR outsourcing arrangement, and/or provides goods or services to aan OSP principal under a CDR outsourcing arrangement using CDR data that it has collected on behalf of the OSP chain principal or that has been disclosed to it by the OSP principal. All OSPs (whether accredited or unaccredited) must comply with the terms of their written contract with the principal that engaged them. As unaccredited OSPs are not bound by the privacy safeguards, these contractual obligations apply in addition to other privacy obligations unaccredited OSPs will have under the Privacy Act if they are APP entities. Where an unaccredited OSP enters a further CDR outsourcing arrangement, that OSP will be the OSP principal under that further arrangement.

A.34 While CDR representatives and unaccredited outsourced service providersOSPs are not directly bound by the Privacy Safeguards set out in Division 5 of Part IVD of the Competition and Consumer Act, they will be party to either a CDR representative arrangement [32] or a CDR outsourcing arrangement[33] as required by the CDR Rules. In accordance with those rules, these written contracts will reflect many of the obligations in the privacy safeguards. This means that, these Guidelines nevertheless contain useful guidance which will be applicable to CDR representatives and unaccredited outsourced service providersOSPs in meeting their contractual obligations.

A.35 In specified circumstances, CDR data can be disclosed outside of the CDR system to unaccredited entities. This includes disclosures to 'trusted advisers', and the disclosuredisclosures to any person under a business consumer disclosure consent, and disclosures of 'CDR insights' to any person. These recipients are not bound by the Privacy Safeguards. However, trusted advisers andthese CDR insightdata recipients should consider any professional or other regulatory obligations they may have in relation to their handling

[32] CDR Rules, rule 1.10AA.

[33] CDR Rules, rule 1.10.

of a consumer's data (including privacy obligations under the Privacy Act if they are an APP entity) and handle data transparently and in the way a consumer would expect.

A.36 Further information on these roles is contained in Chapter B (Key concepts).

Primary and secondary data holders for shared responsibility data (SR data)

A.37 Where the CDR Rules specify CDR data as shared responsibility data (also called SR data in the CDR Rules),[34] some data holders will perform special roles as a primary or secondary data holder for the SR data.

A.38 Primary and secondary data holders, and SR data, are discussed further in Chapter B (Key concepts).

Which privacy protections apply in the CDR context?

CDR entity	Privacy safeguards that apply in the CDR context	APPs that apply in the CDR context
Accredited person	**Privacy safeguards 1–4**[35]	**None. Privacy Safeguards 1–4 apply instead of the corresponding APPs**[36]
Accredited data recipient[37]	**Privacy safeguards 1, 2 and 5–13**	**None. The APPs do not apply to an accredited data recipient of a consumer's CDR data in relation to that data**
Data holder (other than the Australian Energy Market Operator Limited (AEMO))	**Privacy safeguards 1, 10, 11 and 13**	**All APPs (1–13)** **APPs 10 and 13 are replaced by Privacy Safeguards 11 and 13**

[34] See CDR Rules, rule 1.7, and Chapter B (Key concepts) for further information on SR data.

[35] See the Competition and Consumer Act, sections 56EC(4), 56ED, 56EE(1)(b), 56EF and 56EG.

[36] Note: If Privacy Safeguards 1 – 4 do not apply, the corresponding APPs may continue to apply to other handling of the individual's personal information where the accredited person is an APP entity (see the Competition and Consumer Act, subsections 56EC(4) and (5)(aa)). Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See the Privacy Act, subsection 6E(1D).

[37] An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See the Competition and Consumer Act, section 56AK.

CDR entity	Privacy safeguards that apply in the CDR context	APPs that apply in the CDR context
		once the data holder is required or authorised to disclose the CDR data under the CDR Rules
Data holder (AEMO)	**None. AEMO is exempt from the privacy safeguards that otherwise apply to data holders.[38]**	**All APPs (1–13)**
Designated gateway	**Privacy safeguards 1, 6, 7 and 12**	**APPs 1–5, 8–10 and 12–13**

Do the privacy safeguards apply instead of the Privacy Act and the APPs?

A.39 Subsection 56EC(4) of the Competition and Consumer Act sets out when a privacy safeguard applies instead of an Australian Privacy Principle (APP) under the *Privacy Act 1988* (Privacy Act).

A.40 The privacy safeguards apply only to CDR data for which there are one or more CDR consumers.[39]

A.41 As set out in paragraph A.13 above, for there to be a CDR consumer, at least one person must be identifiable or reasonably identifiable from the CDR data or other information held by the relevant entity. As such, where the consumer is an individual, CDR data protected by the privacy safeguards will contain information about an identified or reasonably identifiable individual, and will therefore also be 'personal information' under the Privacy Act.

A.42 To work out when the privacy safeguards apply, an entity needs to consider what capacity they are acting in – as a data holder, accredited person/accredited data recipient, or designated gateway.

A.43 In each chapter in these guidelines, the interaction between the privacy safeguard and corresponding APP is discussed.

[38] In the energy sector, AEMO is exempt from privacy safeguards 1, 11 and 13, and is exempt from privacy safeguard 10 in relation to CDR data held by AEMO that AEMO discloses to an energy retailer as required or permitted by the Competition and Consumer Act: see the Competition and Consumer Regulations 2010 (Competition and Consumer Regulations), sub-regulation 28RA(2). Certain privacy safeguard obligations that would otherwise apply to the AEMO are instead applied to retailers who receive data from AEMO, with some modifications and exceptions: see Competition and Consumer Regulations, sub-regulation 28RA(3)-(4).

[39] Competition and Consumer Act, subsection 56EB(1).

Accredited persons and accredited data recipients

A.44 For an accredited person, or accredited data recipient of CDR data, the privacy safeguards apply instead of the APPs in relation to the handling of the CDR data within the CDR system.[40]

Data holders

A.45 For data holders (other than AEMO), the APPs will apply to CDR data that is also personal information with the exception of APPs 10 (quality of personal information) and 13 (correction of personal information). These two APPs are replaced by Privacy Safeguards 11 (quality of CDR data) and 13 (correction of CDR data) once the data holder is required or authorised to disclose the CDR data under the CDR Rules. Privacy Safeguard 10 (notifying of the disclosure of CDR data) does not have an APP equivalent and applies to data holders in addition to all other privacy protections.

A.46 Data holders (other than AEMO) must also comply with both APP 1 and Privacy Safeguard 1 which relate to open and transparent management of personal information and CDR data respectively. As explained above, these obligations apply concurrently and the obligations in Privacy Safeguard 1 do not displace the APP 1 obligations.

A.47 AEMO is currently the only data holder who is exempt from the Privacy Safeguards that otherwise apply to data holders.[41] The APPs continue to apply to any CDR data held by AEMO that is also personal information.

Designated gateways

A.48 The APPs will continue to apply to designated gateways for CDR data that is personal information except in relation to the use and disclosure of CDR data, including for direct marketing purposes, for which Privacy Safeguards 6 (use or disclosure of CDR data) and 7 (direct marketing) apply instead of APP 6 and APP 7, and the security of the CDR data, for which Privacy Safeguard 12 (security of CDR data) applies instead of APP 11.

A.49 Further, designated gateways must comply with Privacy Safeguard 1 (open and transparent management of CDR data) in addition to APP 1. As explained above, these obligations apply concurrently and the obligations in Privacy Safeguard 1 do not displace the APP 1 obligations.

---

[40] The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data - Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).) Subsection 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa)).

[41] At date of publication. See Competition and Consumer Regulations, regulation 28RA.

Note: *There are currently no designated gateways in the banking sector or energy sector.*[42] *See Chapter B (Key concepts) for the meaning of designated gateway.*

What happens if an entity breaches the privacy safeguards?

A.50 The Information Commissioner has powers to investigate possible breaches of the privacy safeguards, either following a complaint by a consumer who is an individual or small business or on the Information Commissioner's own initiative.

A.51 Where a consumer makes a complaint, the Information Commissioner will generally attempt to conciliate the complaint.

A.52 The Information Commissioner has a range of enforcement powers and other remedies available. These powers include those available under:

- Part V of the Privacy Act,[43] for example the power to make a determination,[44] and
- Part IVD of the Competition and Consumer Act, for example the privacy safeguards attract a range of civil penalties enforceable by the Information Commissioner.[45]

A.53 Where ~~an unaccredited entity (such as~~ a CDR representative or ~~unaccredited outsourced service provider) may have breached privacy-related~~ an OSP breaches their contractual obligations, their CDR representative principal or OSP chain principal ~~under the outsourcing arrangement~~ (as applicable) would be liable and held to have breached the relevant privacy safeguard or related CDR Rule. Such conduct will trigger the Information Commissioner's investigation and enforcement powers against the accredited party, either following a complaint by a consumer who is an individual or small business or on the Information Commissioner's own initiative.

A.54 The ACCC also has a strategic enforcement role where there are repeated or serious breaches. The Office of the Australian Information Commissioner (OAIC) and the ACCC have published a joint Compliance and Enforcement Policy for the CDR intended to help consumers and CDR entities understand the approach that the OAIC and ACCC will take to encourage compliance with the CDR Rules, legislation (including privacy safeguards and

---

[42] For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: Consumer Data Right (Energy Sector) Designation 2020, subsection 6(4). However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in the Competition and Consumer Act, paragraph 56AL(2)(c).

There are also no designated gateways in the telecommunications sector~~,~~ (Consumer Data Right (Telecommunications Sector) Designation 2022) or non-bank lending sector (Consumer Data Right (Non-Bank Lenders) Designation 2022), although unlike the banking and energy sectors, at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data or non-bank lending data under the CDR system~~: Consumer Data Right (Telecommunications Sector) Designation 2022~~.

[43] The Competition and Consumer Act, subsection 56ET(4),~~-~~ extends the application of Part V of the Privacy Act to a privacy safeguard breach relating to the CDR data of a consumer who is an individual or small business.

[44] Privacy Act, section 52.

[45] Competition and Consumer Act, section 56EU. All privacy safeguards contain civil penalty provisions except for Privacy Safeguard 2.

Consumer Data Standards) and how they will respond to breaches of the regulatory framework. The OAIC has also published a CDR Regulatory Action Policy which sets out the OAIC's priorities, goals and principles in regulating the CDR, and complements the joint Compliance and Enforcement Policy.

Where do I get more information?

A.55 The OAIC has further information about the CDR and its role on the OAIC website, see www.oaic.gov.au/consumer-data-right.